AMENDMENT TO THE CLAIMS

This listing of the claims replaces all prior versions and listings of the claims in the application.

1.   (Currently Amended) A method comprising:

analyzing a plurality of database access statements that were issued for an application ~~in~~ during use[[;]] to determine previous ~~determining~~ accessed items and types of access for the application ~~based on the issued database access statements for the application~~; and

developing a role ~~associated with~~ for the application based on the previous ~~determined~~ accessed items and types of access for the application, wherein ~~the role allows a user database access~~ when ~~the user is associated with~~ the application is in use by a user, the developed role for the application allows the user database access.

2.   (Currently Amended) The method of claim 1 wherein analyzing the issued database access statements comprises:

capturing the plurality of database access statements;

normalizing the captured database access statements; and

eliminating redundancies in the normalized database access statements.

3.   (Original) The method of claim 2 wherein the database access statements comprise Structured Query Language (SQL) queries.

4.   (Currently Amended) The method of claim 1 wherein the ~~determined~~ previous accessed items and types of access include objects accessed and operations performed on the objects.

5.   (Currently Amended) The method of claim 1 wherein developing a role comprises determining permissions for the application based on the ~~determined~~ previous accessed items and types of access.

Applicant : John D. Richter   Attorney's Docket No.: 14012-053001 / 50-03-034
Serial No. : 10/736,001
Filed   : December 15, 2003
Page   : 3 of 9

6.   (Original) The method of claim 1 further comprising determining which of a set of users are authorized to use the application.

7.   (Currently Amended) The method of claim 1 further comprising:

         detecting a user request to establish an application session;

         finding the role ~~associated with~~ <u>for</u> the application; and

         assigning the role to a user.

8.   (Original) The method of claim 7 wherein detecting a user request to establish an application session comprises determining if a user is authorized to use the application.

9.   (Original) The method of claim 7 further comprising:

         detecting an end of the application session; and

         if an end of the application session is detected, disabling the assigned role for the user.

10. (Currently Amended) An article comprising a machine-readable medium storing instructions operable to cause one or more machines to perform operations comprising:

analyzing a plurality of database access statements that were issued for an application in during use[[;]] to determine previous determining accessed items and types of access for the application based on the issued database access statements for the application; and

developing a role associated with for the application based on the previous determined accessed items and types of access for the application, wherein the role allows a user database access when the user is associated the application is in use by a user, the developed role for the application allows the user database access.

11. (Currently Amended) The article of claim 10, wherein analyzing the issued database access statements comprises:

determining whether the plurality of database access statements have been captured;

normalizing the captured database access statements; and

eliminating redundancies in the normalized database access statements.

12. (Currently Amended) The article of claim 10 wherein the previous determined accessed items and types of access include objects accessed and operations performed on the objects.

13. (Currently Amended) The article of claim 10 wherein developing a role comprises determining permissions for the application based on the previous determined accessed items and types of access.

14. (Original) The article of claim 10 wherein the instructions are further operable to cause one or more machines to perform operations comprising determining which of a set of users are authorized to use the application.

15. (Currently Amended) The article of claim 10 wherein the instructions are further operable to cause one or more machines to perform operations comprising:

determining whether a user request to establish an application session has been detected;

finding the role ~~associated with~~ <u>for</u> the application; and

assigning the role to a user.

16.   (Original) The article of claim 15 wherein detecting a user request to establish an application session comprises determining if a user is authorized to use the application.

17.   (Original) The article of claim 15 wherein the instructions are further operable to cause one or more machines to perform operations comprising:

detecting an end of the application session; and

if an end of the application session is detected, disabling the assigned role for the user.

Applicant : John D. Richter   Attorney's Docket No.: 14012-053001 / 50-03-034
Serial No. : 10/736,001
Filed   : December 15, 2003
Page   : 6 of 9

18.   (Currently Amended) A database security analyzer comprising:

     a communication interface operable to receive a plurality of database access statements that were issued for an application ~~in~~ during use;

     a memory operable to store the issued database access statements; and

     a processor operable to develop a role ~~associated with~~ for the application based on the previously issued database access statements for the application, wherein when the application is in use by a user, the developed role for the application allows a user database access ~~when using the application~~.

19.   (Currently Amended) The analyzer of claim 18 wherein developing a role comprises:

     analyzing the database access statements to determine previous ~~determining~~ accessed items and types of access for ~~an~~ the application ~~based on the issued database access statements for the application~~;

     determining permissions for the application based on the previous ~~determined~~ accessed items and types of access for the application; and

     developing a role associated with the application based on the determined permissions.

20.   (Currently Amended) The analyzer of claim 19 wherein the previous ~~determined~~ accessed items and types of access include objects accessed and operations performed on the objects.

21.   (Currently Amended) The analyzer of claim 18 wherein developing a role comprises:

     determining whether ~~issued~~ the received database access statements have been captured;

     normalizing the captured database access statements; and

     eliminating redundancies in the normalized database access statements.

22.   (Original) The analyzer of claim 18 wherein the memory comprises instructions, and the processor operates according to the instructions.

23.   (Currently Amended) A method comprising:

capturing the a plurality of database access statements that were issued for one or more applications in during use, wherein the database access statements comprise Structured Query Language (SQL) queries;

normalizing the issued captured database access statements;

eliminating redundancies in the normalized database access statements;

analyzing the normalized database access statements to determine previous determining accessed items and types of access for an application based on the issued database access statements for the application, wherein the previous determined accessed items and types of access include objects accessed and operations performed on the objects;

determining permissions for the application based on the previous accessed items and types of access for the application;

developing a role associated with for the application based on the developed determined permissions;

determining which of a set of users are authorized to use the application;

detecting a user request to establish a session of the application;

determining if the user is authorized to use the application;

if the user is authorized to use the application, finding the role associated with for the application;

assigning the role to the user;

detecting an end of the application session; and

if an end of the application session is detected, disabling the assigned role for the user.